AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

NHA House #5, Cudei, New Mexico
GPS Coordinates 36.834931,-108.758468

Case No. **22 MR 1383**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §1153 & 2242 (2)	Sexual abuse committed in Indian Country

The application is based on these facts:

See attached affidavit, submitted by SA Nicole Montgomery and approved by AUSA Novaline Wilson

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nicole Montgomery, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephonically sworn and electronically signed *(specify reliable electronic means)*.

Date: September 16, 2022

Judge's signature

City and state: Farmington, NM

B. Paul Briones, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: NHA House #5, Cudei, New Mexico, GPS Coordinates 36.834931,-108.758468	Case No.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Nicole Montgomery, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the search of Navajo Housing Authority (NHA) House #5, Cudei, New Mexico (GPS coordinates 36.834931,-108.758468) (hereafter referred to as the "SUBJECT PREMISES"), as further described in Attachment A (incorporated herein by reference) for the items described in Attachment B (incorporated herein by reference).

2. I am "an investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

3. I am a Special Agent with the Federal Bureau of Investigation and have been employed as such since 2017. I am currently assigned to the Albuquerque Division, Farmington Resident Agency, which is responsible for investigating violent crimes occurring in Indian Country, including robbery, aggravated assaults, assaults on federal officers, sexual assaults, and

homicides, as well as crimes involving children, including the production, distribution, and receipt of child pornography and kidnapping. I have eight years of prior law enforcement experience working as a police officer in the State of Illinois and as a detective in the Commonwealth of Virginia. Additionally, I attended three separate law enforcement academies and completed multiple in-service training courses relating to my duties.

4. I have received on the job training from other experienced agents and law enforcement officers. My investigative training and experience includes, but is not limited to, conducting surveillance, interviewing subjects, writing affidavits for search and arrest warrants, collecting evidence and learning legal matters which includes the topics of fourth amendment searches.

5. The following information contained in this affidavit is based on my training and experience, my personal participation in this investigation, and information provided to me by other law enforcement officials. Unless otherwise indicated, where I have referred to written or oral statements, I have summarized them in substance and in part, rather than verbatim. Not all of the facts of the investigation known to me are contained herein, only those necessary to establish probable cause to search the below-listed items pertaining to the captioned investigation.

6. As will be shown below, there is probable cause to believe that the SUBJECT PREMISES will provide evidence of violations of 18 U.S.C. §§ 2242(2) and 1153 (Sexual Abuse in Indian Country) (hereinafter referred to as the "TARGET OFFENSES"). Based on the facts set forth in this affidavit, there is probable cause to believe that the TARGET OFFENSES were committed by Durward Deale, year of birth (YOB) 1980 (hereinafter referred to as "Deale"), an enrolled member of the Navajo Nation Indian Reservation, who resides at the SUBJECT PREMISES.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, acts or omissions in furtherance of the offenses under investigation occurred within Indian Country in the District of New Mexico. *See* 18 U.S.C. § 1153.

DEFINITIONS

8. The following terms are relevant to this affidavit in support of this application for a search warrant:

a. *Computer*: The term "computer" refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, mobile phones, and devices. *See* 18 U.S.C. § 1030(e)(1).

b. *Computer Hardware*: The term "computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and

related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

c. *Computer passwords and data security devices*: This term consists of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

d. *Electronic mail ("e-mail" or "email")*: "E-mail" refers to a method of exchanging digital messages from an author to one or more recipients. Users may attach digital media to their e-mails. Modern e-mail operates across the Internet or other computer networks. E-mail systems are based on a store-and-forward model. E-mail servers accept, forward, deliver and store messages. E-mail accounts may be accessed by computers, to include smartphones and tablets.

e. *File Transfer Protocol ("FTP")*: FTP is a standard network protocol used to transfer computer files from one host to another over a computer network, such as

the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

f. *Hash Value*: A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

g. *Internet*: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. *Internet Protocol ("IP") Address*: An "IP address" is a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a

particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

i. *Internet Service Providers ("ISPs")*: "ISPs" are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. *Smartphone*: A "smartphone" is a type of mobile or cellular telephone, and functions as multi-purpose mobile-computing devices. Smartphones can function as traditional telephones with the additional ability to store contact information, send and receive voice, text, and media messages, store information and media, access the Internet, and perform many of the same functions as a traditional computer. A smartphone user may perform these various functions through software applications ("apps") which may store evidence of such use on the device.

k. "*Records*," "*documents,*" *and* "*materials*": These terms include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. *Visual Depictions*: "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

PROBABLE CAUSE

9. On September 13, 2022, the Sexual Assault Services (SAS) of New Mexico (NM) contacted the FBI regarding the sexual assault of C.N., YOB 1985 (hereinafter referred to as "Jane Doe," an enrolled member of the Navajo Nation), on September 11, 2022. Jane Doe alleged that her ex-common law husband, Deale, sexually assaulted her in her sleep in their shared residence, located at NHA House #7, Newcomb, NM (GPS coordinates 36.284013,-108.707237), which is located within the exterior boundaries of the Navajo Nation Indian Reservation. Jane Doe was interviewed by the FBI on September 13, 2022.

10. According to Jane Doe, she and Deale began a dating relationship in 2005 and dated on and off until 2012. Deale was mentally and emotionally abusive toward Jane Doe in the beginning, and it eventually escalated to physical violence. During their relationship, Deale would secretly photograph and video record them having consensual sex. Jane Doe only discovered he was doing this after looking through his phone and finding photographs and videos. She would also catch Deale watching pornography on his phone while having sex with her. Jane Doe believed Deale had an addiction to pornography, as she would find "jump" drives containing numerous pornographic images, meticulously organized by year and porn star. She and Deale would argue about his pornography collection, and it would often lead to them breaking up, only to later get back together.

11. Jane Doe and Deale had two children together and filed paperwork with the Navajo Nation to become married via common law. Anytime Jane Doe and Deale separated, he would take the children from Jane Doe. They separated in 2017 after Jane Doe found the "jump" drives containing pornography. In 2019, Jane Doe was approved for NHA housing and moved into her house in Newcomb. She asked Deale if the children could move in with her. Deale

agreed, but only if he could move in, as well. Jane Doe had her own bedroom and Deale would sleep in the living room on the couch. They attempted throughout the years to reconcile, but it never lasted. Deale continued to live with Jane Doe and their children, but for the past six months, Jane Doe has not consented to sex with Deale.

12. On May 16, 2022, Jane Doe woke up with pain in her vagina, feeling like she had sex. On May 17, she woke up again feeling like she had sex, with accompanied bleeding from her vagina. On May 18, she woke up and used the bathroom. She had pain when she urinated, and upon further inspection, located a scratch on her vagina. On May 19, she awoke again feeling like something happened to her. Jane Doe was not sexually active with anyone during this time period, and had not been sexually active with Deale for several months.

13. On May 20, 2022, Jane Doe, Deale, and their two children went to Pizza Hut in Farmington, NM to pick up dinner. While waiting, their son was playing on Deale's unlocked iPhone. When Deale went inside to get the pizza, Jane Doe took the opportunity to look in Deale's phone. She found photographs and a video of her naked body. In the video and images, Jane Doe was lying face down, naked on her bed. The video showed a hand touching Jane Doe's buttocks. Jane Doe identified her body and recognized Deale's hand in the video. The photographs showed object placed on her buttocks, such as two plush toys belonging to the children. Other photographs showed Jane Doe wearing a thong that she did not put on prior to going to sleep. Jane Doe confronted Deale about the contents of her phone. He told her the images she saw were from the fifth time he touched her in her sleep, and that he had done it to her four times prior. According to Jane Doe, she has always been a heavy sleeper, and she would take melatonin, which would put her into an even deeper sleep.

14. On July 17, 2022, Jane Doe returned home from a camping trip. She drank alcohol at home before going to sleep alone in her bed. The next morning, she woke up and used the bathroom. Her vagina hurt and it felt like she had sex the night prior. She looked down at her underwear and saw she was wearing a backwards thong. She had gone to sleep in a different pair of underwear. When she confronted Deale about it, he told her that he was rubbing her feet and she smelled like urine so he changed her underwear. Jane Doe questioned why he changed her underwear and not her shorts, if she truly peed on herself. On July 20, 2022, Jane Doe began bleeding from her vagina again. She took a photograph of the bloody toilet paper and confronted Deale with it, as she is on birth control and no longer gets periods. In a text message exchange, Deale denied having sex with her, but said, "I rubbed you lower body is all."

15. Approximately one month ago, around the beginning of August 2022, Jane Doe went through her daughter's Apple iPad to make sure she was not doing anything inappropriate. In the photos folder, she found and viewed a video of Deale touching her (Jane Doe).

16. On September 11, 2022, Jane Doe, Deale, and their family had dinner together. Jane Doe and Deal consumed alcohol. Jane Doe drank approximately three mixed drinks and two glasses of wine. Just before 9:00 p.m., she went to sleep in her bedroom with her juvenile son. Deale followed her to her room to rub her feet, as she suffers from foot issues. Foot massages are not considered sexual foreplay for Jane Doe and Deale and has never led to sex. Jane Doe fell asleep on her stomach while Deale rubbed her feet.

17. Jane Doe, still in a drowsy state after being asleep and consuming alcohol, felt movement on the bed. Her son was no longer in the room. As she lay on the bed, Jane Doe felt Deale put liquid on her vagina, insert his finger into her vagina, and then insert his penis two times into her vagina. She also saw a flash, as if a photograph or video was taken of her. He then

pulled off a thong that Jane Doe was not previously wearing. He wiped her vagina with a baby wipe and lied down on the bed next to her abruptly since Jane Doe started to move. Jane Doe described that these events transpired quickly. Jane Doe, now fully alert, mounted Deale, choked him, and threatened to kill him if he ever touched her again. They continued to verbally argue, with Deale telling her that she "set him up." Jane Doe kicked him out of her bedroom after they stopped arguing. She text messaged him at 12:40 a.m. telling him it was not okay for him to rape her and that he could not stay at her house anymore. He did not respond.

18. The next morning, Jane Doe found the white thong, baby oil, baby wipes, and Deale's cell phone in her bedroom. She photographed most of the objects. Jane Doe had a sexual assault examination later that day in Gallup, NM. After returning home, she discovered Deale had cleaned her bedroom, either hiding or taking with him the baby oil and white thong. He and the children went to Deale's parents' house (the SUBJECT PREMISES), located at NHA House #5, Cudei, NM (GPS coordinates 36.834931,-108.758468). Whenever Deale is not staying with Jane Doe at her house in Newcomb, NM, he stays at the SUBJECT PREMISES, as he does not work and does not have the financial means to rent his own house or apartment.

19. Deale is in possession of an Apple iPhone, an Apple iPad, and an Apple iPad mini. He may have other electronic devices with him that Jane Doe does not know about. According to Jane Doe, Deale is also in possession of a blue Chevrolet Malibu. Deale, in fact, has a blue Chevrolet Malibu, bearing New Mexico license plate 366TWT and vehicle identification number ("VIN") 1G1ZC5E19BF271578, registered to him. The vehicle was spotted at the SUBJECT PREMISES on September 14, 2022 by law enforcement.

BACKGROUND ON COMPUTERS AND THE INTERNET

20. I have both training and experience in the investigation of computer-related crimes. Based on my training and knowledge, I know the following:

a. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs and/or videos.

b. A device known as a "modem" allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections.

c. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which plug into a port on a computer or tablet, either directly or through the use of an external disc drive or port adapter – can store thousands of images and/or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer or tablet, and then copy it (or any other files on the computer or tablet) to any one of those media storage devices.

d. Individuals also use online resources to retrieve and store photographic evidence. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find photographic evidence on the user's computer, smartphone or external media in most cases.

OFFENDER CHARACTERISTICS

21. Based on my previous investigative experience related to sexual assault investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who create and/or possess photographic evidence of their crimes:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from having sexual contact with persons who are unable to consent to the sexual contact, or from fantasies they have viewing non-consenting persons in sexually suggestive poses, such as in person or in photographs.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media.

c. Such individuals often maintain their pornography material in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. This pornography material is often maintained for several

years and kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the pornography images at leisure.

d. Importantly, evidence of such activity, including deleted pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals often transfer electronic files containing pornography from device to device, either to make room on their devices, or for long-term storage.

22. I also know from training and experience that some persons who create and/or possess pornography or photographic evidence of their sexual crimes engage in "collector behavior." Persons who are "collectors" of pornography or photographic evidence of their sexual crimes often keep the material in their possession for years, because it is considered valuable to them. They may receive sexual gratification, stimulation, and satisfaction from reviewing the photographs and videos they created. Given Deale's history of downloading and saving pornographic images retrieved from the Internet to external devices, such as "jump" drives, I believe he exhibits "collector" behavior.

BIOMETRIC ACCESS TO DEVICES

23. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric

passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

a. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

b. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

c. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to

access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request permission to: (1) press or swipe the fingers (including thumbs) of Deale to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the face of Deale and activate the facial recognition

feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of Deale and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that Deale state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to ask Deale to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices

CONCLUSION

24. Based on the information set forth above, there is probable cause to believe that items more fully described in Attachment B and consisting of evidence, contraband, instrumentalities and/or fruits of violations of 18 U.S.C. §§ 2242(2) will be found at the location more fully described in Attachment A. Further, based upon the foregoing paragraphs, judicial authority is specifically requested to complete the search/examination of the seized items at an appropriate law enforcement facility.

25. Assistant United States Attorney Novaline Wilson has reviewed and approved this search warrant application.

26. I swear that this information is true and correct to the best of my knowledge.

Respectfully submitted,

Nicole Montgomery
Special Agent
Federal Bureau of Investigation

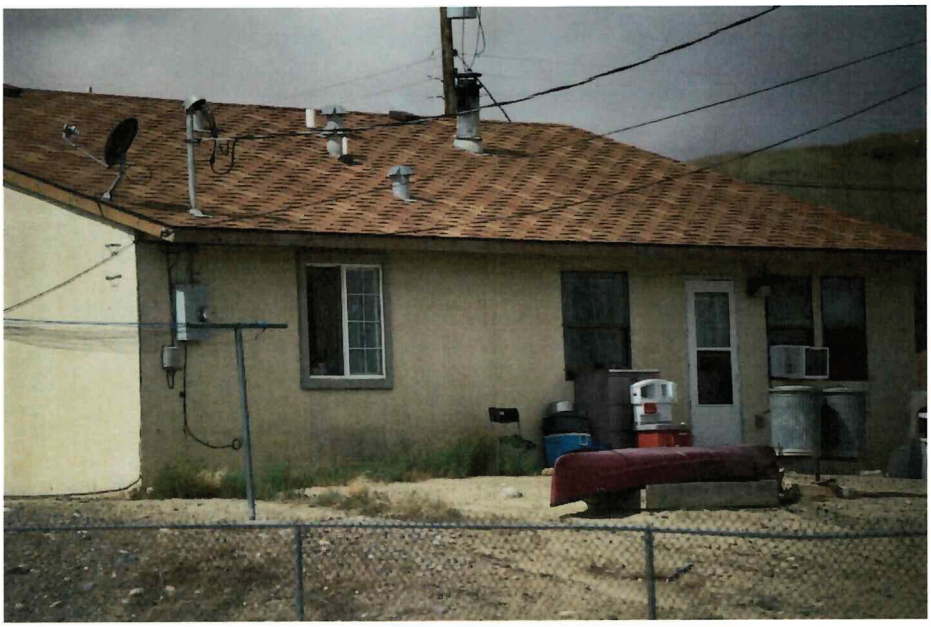
Telephonically sworn and electronically signed on this 16th day of September, 2022.

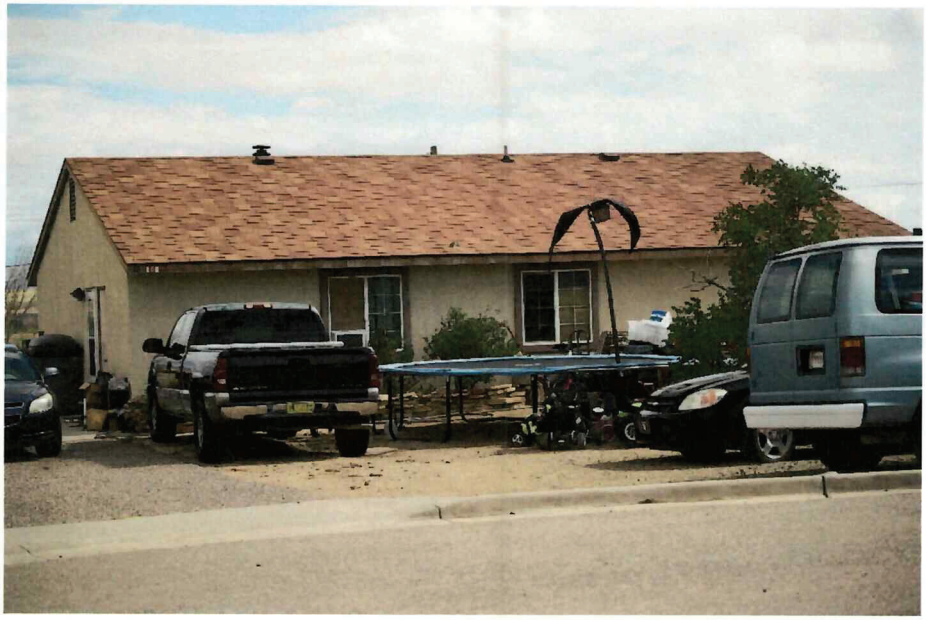
B. Paul Briones
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is described as follows:

1. The entire property located at Navajo Housing Authority ("NHA") House #5, Cudei, NM in vicinity of GPS coordinates 36.834931,-108.758468, including the residential building, any outbuildings, any appurtenances, and the surrounding curtilage ("SUBJECT PREMISES"). The property may be described as a single-family residence with beige exterior walls and brown roof shingles.





2. A blue Chevrolet Malibu, New Mexico license plate 366TWT, vehicle identification number ("VIN") 1G1ZC5E19BF271578.

3. The person of DURWARD DEALE (DOB: 08/17/1980), provided that this person is located at the subject premises and/or within the District of New Mexico at the time of the search.

4. During the execution of the search of the premises described in Attachment A, law enforcement personnel are also specifically authorized to compel DEALE to provide biometric features, including pressing fingers (including thumbs) against and/or putting a device in front of a face, or any other security feature requiring biometric recognition, of:

    a. any of the devices found at the premises, and
    b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the premises to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device.

This warrant does not authorize law enforcement personnel to require that DEALE state or otherwise provide the password or any other means that may be used to unlock or access

the devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

ATTACHMENT B

The following materials, which constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended to use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2242(2) and 1153:

1. Computers or storage media used as a means to commit the violations described above.

2. All visual depictions (including images, videos, negatives, still photos, video tapes, artists drawings, slides and any type of computer formatted file) which depict Jane Doe engaged in sexual conduct, or the lewd exhibition of genitalia, or posed or candid in a sexual manner, including clothed or partially clothed.

3. All documentation related to computer passwords, encryption keys, and other access devices.

4. All computer hardware equipment, connector cables, and corresponding logs (including: central processing units, monitors, modems, routers, keyboards, printers, computer scanner equipment and or video transfer equipment).

5. All storage devices (including: external and internal hard drives, cell phones, "smart" phones, and PDA's capable of sending and receiving images and/or text messages, thumb drives, cartridge tapes, magnetic tapes, optical and digital storage devices, digital cameras, CD's, DVD's, memory cards, Micro SD Cards, iPods, X-Box, PSP players, video game consoles, floppy disks or other media capable of storing data).

6. All computer software stored on hard disks, digital, optical, and magnetic media devices, and floppy disks containing computer programs, including software data files, electronic mail files, instant message files, software programs and files to receive and or transmit photographs, and operating logs and instruction manuals relating to the operation of the computer hardware and software to be searched.

7. All computer related manuals, textbooks, computer print outs, and other documents used to access computers and record information taken from computers.

8. Articles of personal property tending to establish the identity of person or persons having the dominion and control over the computer equipment, cellular telephone, or digital media.

9. All evidence related to all off-site storage units, other residences, safety deposit boxes, etc. where diaries, notes, journals, pictures or other evidence of sexual crimes may be stored for safekeeping against seizure.

10. Any and all clothing belonging to Jane Doe, included but not limited to thong-style underwear.

11. Baby oil or other lubricants.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.